FortiAuthenticator - Two-Factor Authentication for Web Applications Solution Guide

VERSION 1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

7/7/2016

FortiAuthenticator 4.1 - Two-Factor Authentication for Web Applications Solution Guide

23-410-378944-20160706

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-07-06	Initial release.

Introduction

The weak policy of only User Name and Password as credentials for authentication to a website results in a system vulnerable to unauthorized access. Website login must be enhanced to use a strong authentication method. Two-Factor Authentication (2FA), using One Time Passwords (OTP), is one of the most secure and strong authentication solutions, while being the easiest to implement, and having the lowest associated cost.

This document provides details, along with specific examples, of how to add 2FA to your web application using FortiToken Mobile and FortiAuthenticator.

Overview

This solution guide describes how to use the FortiAuthenticator (FAC) Application Programming Interface (API) for integration of 2FA with a generic web application. The API is based on FAC version 4.1.

The second factor OTP is generated on either a hardware or software token, or can be delivered to the end user via email or SMS. This guide deals only with FortiToken Mobile software tokens as the OTP generators, which have the advantage of being able to deploy to an unseen user base. But the solution can be easily modified to use other methods with the same FAC API.

There are many other possible variations to the solution besides token type depending on the specific needs of the organization. Some of the key variables to consider are:

- Local User versus Remote User – local users are provisioned directly on the FAC while remote users are imported and synchronized from a remote LDAP or AD server
- Local Users and Remote Users have several options for validating the first factor:
  - Don't require first factor – use OTP only
  - Website validates user first factor independent of FAC
  - FAC validates user first factor before verifying OTP
- OTP token activation notification messages can be sent to the end user via email or SMS

Each variation has a slightly different flow. The example flow included in this solution guide is for the case where the user is a remote user imported from LDAP to FAC and the first factor is validated by the website login page directly against LDAP.

Login Design

The login behavior is represented in the three flowcharts presented in this section. The steps in the flow charts are numbered for reference but do not necessarily represent sequential order of operations.

Any step that makes an API call is followed up in the next section with a sample API call and relevant response.

You will need the API username from FAC and API key to use the FAC APIs specified here.

Administrative access to FAC Web Management UI is needed to configure relatively static parameters for which there is no API control.

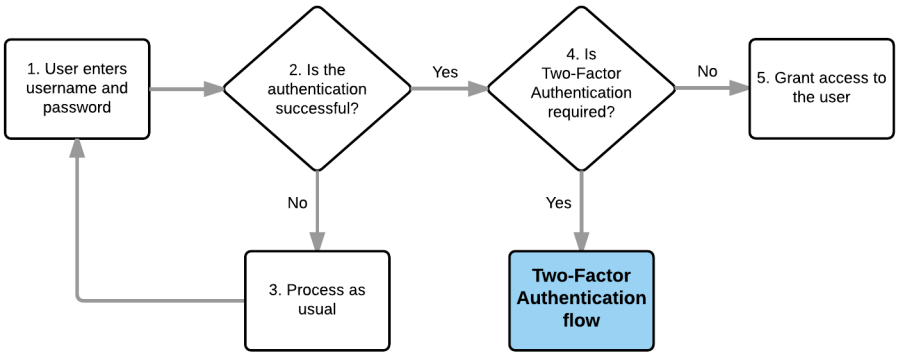
The complete FortiAuthenticator 4.1 Administration Guide can be found here:
http://docs.fortinet.com/d/fortiauthenticator-4.1-administration-guide

The complete FortiAuthenticator REST API Solution Guide can be found here:
http://docs.fortinet.com/d/fortiauthenticator-rest-api-solution-guide-3

Some modifications to your web app login UI will be required. A sample logical flow for a generic web application login procedure using the FAC API is specified in this section.

Flowchart 1: Determine if 2FA is required (optional)

While FAC today does not support native risk-based authentication (also called adaptive authentication), you can modify your web app to decide whether to enforce 2FA based on certain variables. For example, you can white list all your internal IP addresses and then have your application invoke the 2FA authentication, only if the user is not attempting to access the web application from an internal IP address. The flowchart below shows the initial login attempt where the user supplies the first set of credentials, in this case, a username and static password.



In this example, we assume the Remote User case where the web application validated the username and password independently of FAC.

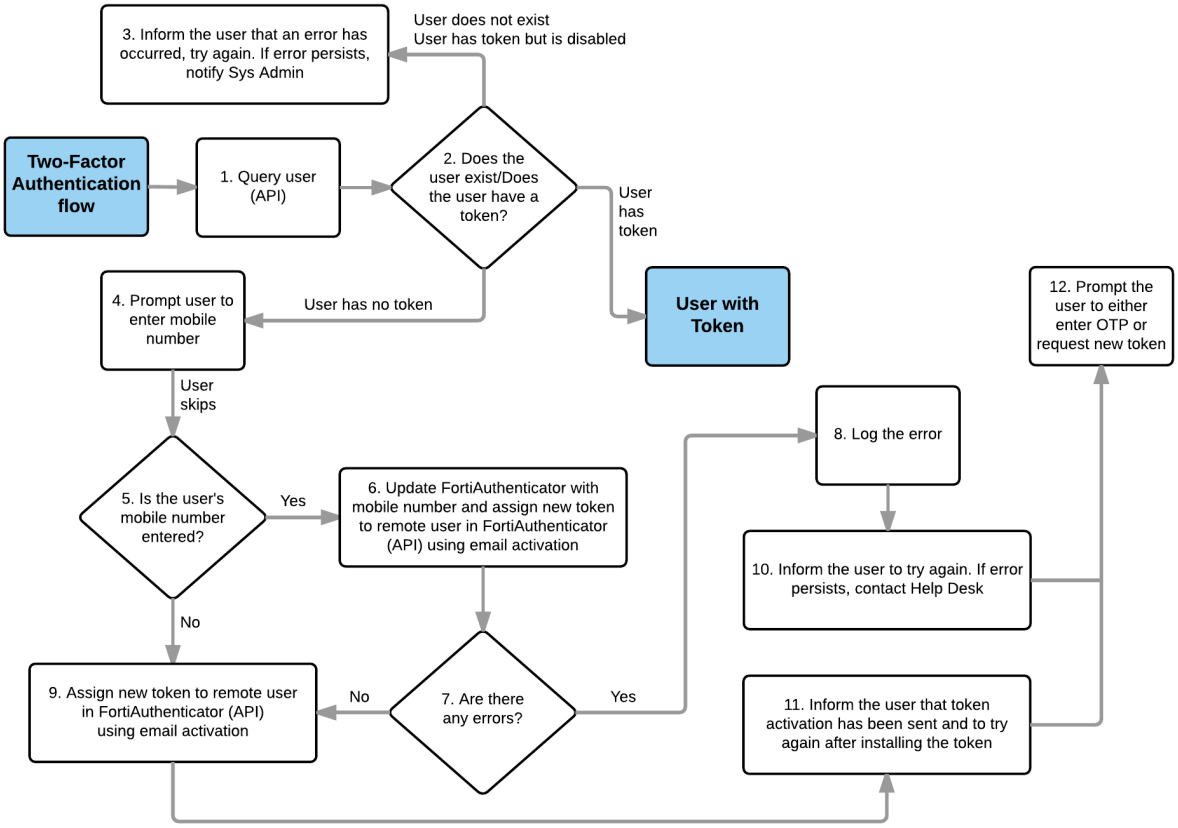
1. Start with user entering their username and password.
2. Verify username and password against pre-existing user base.
3. Then check to see if 2FA is required for this login attempt (Step 4).

4. If 2FA is not required, then grant end user access (Step 5).
5. If 2FA is required, then proceed to **Two-Factor Authentication flow** in Flowchart 2 below.

Flowchart 2: 2FA required and user has no Token

In this example the first time token activation notification is sent via email. The user is asked to enter mobile number if they want to use self service from this site in the future to get a new token (e.g. reset or replace their mobile device).

The reason that subsequent token activations for a given user are delivered via SMS is to prevent an unauthorized user that has stolen or guessed the user name and password from also obtaining the token. This would be possible if activation was sent via email in the case where the username and password were that same credentials as for email access or directory access.

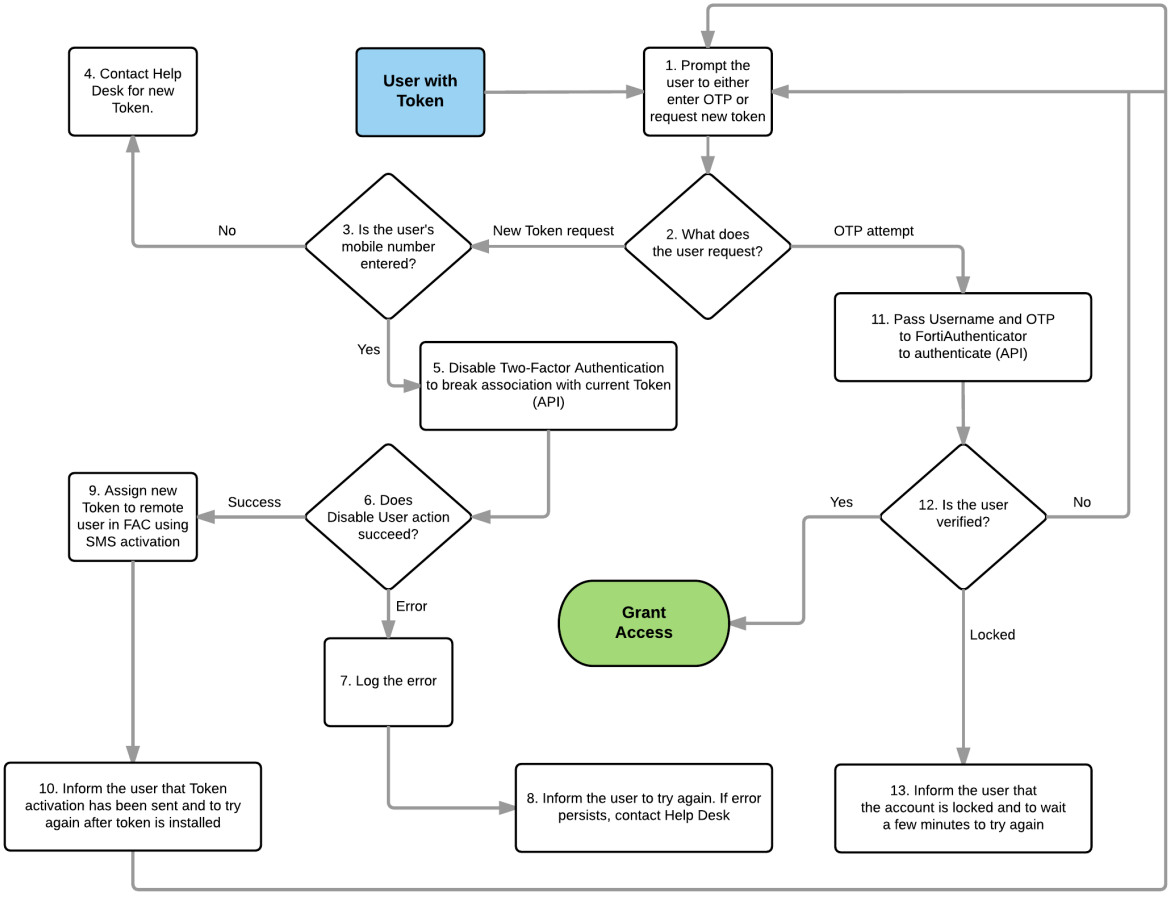


1. Upon determining 2FA is required for end user, query user in FAC.
2. Determine FAC user status.
3. If user does not exist in FAC or is disabled in FAC, display error.
4. If user already has a token assigned in FAC, then proceed to Flowchart 3: 2FA required and user has a Token below (User with Token).
5. If user exists and has no token, prompt user to enter mobile number for future access to self-service token activation (Step 4). This part of the flow is optional. You can also first check if the mobile number is already populated in FAC (Step 5), in which case it can be presented to the user for verification.
6. If user enters mobile number, store it to FAC.
7. Check for errors.

8. If error is returned, log the error.
9. If mobile number update succeeds, then assign new token to user.
10. If user skips entering mobile number, then assign new token to user (Step 9).
11. If assignment fails, log error (Step 8) and inform user to try again (Step 10).
12. Inform user that token was assigned and to check email for activation code (Step 11).
13. Prompt user to enter OTP or Request New Token (Step 12).

Flowchart 3: 2FA required and user has a Token

In this example, if it is not the first time the user has been assigned a token, then requesting a new token can only be done if a mobile number was previously recorded in FAC. This is for security reasons, as explained previously.



1. Prompt user with token to Enter OTP or Request new Token.
2. Determine user request.
3. If new token is requested, check if user's mobile number is in FAC–This is known from the result of the user query in Step 1 of Flowchart 2: 2FA required and user has no Token above.
4. If mobile number is not in FAC, inform user to contact the FAC administrator.
5. If mobile number is in FAC, then disable the 2FA to unassign token in FAC.
6. If user disable action fails, log error (Step 7) and inform user to try again (Step 8).

7. If user disable action succeeds, inform user that token was assigned and to check email for activation code (Step 10).
8. If the user is entering OTP for second factor authentication (Step 2), then pass the username and OTP to FAC for verification (Step 11).
9. Determine verification results (Step 12).
10. If verification fails, re-prompt user (Step 1).
11. If verification succeeds, grant user access (Grant Access).
12. If user is locked, then inform user to wait and try again later (Step 13). This assumes that you have set up FAC to lock a user after a specified number of invalid attempts in FAC.
13. Prompt user to enter OTP or Request New Token (Step 1).

Sample API Calls

Refer to step numbering on Flowcharts above.

Step 1 in Flowchart 2: Query User

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -H 'ACCEPT:' "https://172.30.71.174/api/v1/ldapusers/?format=json&username=davidr"

Response: User with Id 8 exists and has token - go to Step 1 in Flowchart 3

{"meta": {"limit": 20, "next": null, "offset": 0, "previous": null, "total_count": 1}, "objects": [{"active": true, "dn": "CN=david r,CN=Users,DC=vm-lab,DC=vm-eb,DC=com", "email": "dredberg@fortinet.com", "first_name": "david", "ftm_act_method": "email", "ftm_auth_method": "", "id": 8, "last_name": "r", "mobile_number": "+1-6507142203", "resource_uri": "/api/v1/ldapusers/8/", "server_address": "172.30.68.122", "server_name": "PM-LAB-DC", "token_auth": true, "token_serial": "FTKMOB5B62653422", "token_type": "ftm", "username": "davidr"}]}

Response: User with Id 6 has no token - go to Step 4 in Flowchart 2

{"meta": {"limit": 20, "next": null, "offset": 0, "previous": null, "total_count": 1}, "objects": [{"active": true, "dn": "CN=David Redberg,CN=Users,DC=vm-lab,DC=vm-eb,DC=com", "email": "", "first_name": "David", "ftm_act_method": "email","ftm_auth_method": "", "id": 6, "last_name": "Redberg", "mobile_number": "+1-6507142203", "resource_uri": "/api/v1/ldapusers/6/", "server_address": "172.30.68.122", "server_name": "PM-LAB-DC", "token_auth": false, "token_serial": "", "token_type": "", "username": "david"}]}

Response: User does not exist in FAC - go to Step 3 in Flowchart 2

{"meta": {"limit": 20, "next": null, "offset": 0, "previous": null, "total_count": 0}, "objects": []}

Response: User is disabled in FAC - go to Step 3 in Flowchart 2

{"meta": {"limit": 20, "next": null, "offset": 0, "previous": null, "total_count": 1}, "objects": [{"active": false, "dn": "CN=david r,CN=Users,DC=vm-lab,DC=vm-eb,DC=com", "email": "dredberg@fortinet.com", "first_name": "david", "ftm_act_method": "email", "id": 8, "last_name": "r", "mobile_number": "+1-6507142203", "resource_uri": "/api/v1/ldapusers/8/", "se rver_address": "172.30.68.122", "server_name": "PM_LAB_DC-122", "token_auth": false, "token_serial": "", "token_type": "", "username": "davidr"}]}

Step 5 in Flowchart 3: Disable 2FA to break association with current token

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -X PATCH -d " {\"active\":\"false\",\"ftk_only\":\"true\",\"token_auth\":\"false\"}" -H "Content-Type:application/json" https://172.30.71.174/api/v1/ldapusers/8/"

Response: Success

{"active": false, "dn": "CN=david r,CN=Users,DC=vm-lab,DC=vm-eb,DC=com", "email": "dredberg@fortinet.com", "first_name": "david", "ftk_only": "true", "ftm_act_method": "email", "ftm_auth_method": "", "id": 8, "last_name": "r", "mobile_number": "+1-6507142203", "resource_uri": "/api/v1/ldapusers/8/", "server_address":

"172.30.68.122", "server_name": "PM-LAB-DC", "token_auth": false, "token_serial": "", "token_type": "", "username": "davidr"}

Step 9 in Flowchart 3: Assign new Token to Remote User using SMS activation

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -X PATCH -d "{\"active\":\"true\",\"ftk_only\":\"true\",\"token_auth\":\"true\",\"token_type\":\"ftm\",\"ftm_act_method\":\"sms\"}" -H "Content-Type:application/json" https://172.30.71.174/api/v1/ldapusers/8/"

Response: Success

{"activation_code": "DEICYGKYWGO7IWEG", "active": true, "dn": "CN=David Redberg,CN=Users,DC=vm-lab,DC=vm-eb,DC=com", "email": "dredberg@fortinet.com", "first_name": "David", "ftk_only": "true", "id": 6, "last_name": "Redberg", "mobile_number": "", "resource_uri": "/api/v1/ldapusers/6/", "server_address": "172.30.68.122", "server_name": "PM_LAB-DC-122", "token_auth": true, "token_serial": "FTKMOB5A1667E477", "token_type": "ftm", "username": "david"}* Connection #0 to host 172.30.71.174 left intact

Step 6 in Flowchart 2: Update FAC with mobile number and assign new Token to remote User using email activation

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -X PATCH -d "{\"active\":\"true\",\"ftk_only\":\"true\",\"token_auth\":\"true\",\"token_type\":\"ftm\", \"mobile_number\": \"+1-6507142203\",\"ftm_act_method\":\"email\"}" -H "Content-Type:application/json" https://172.30.71.174/api/v1/ldapusers/8/"

Step 9 in Flowchart 2: Assign new Token to remote user in FAC using email activation

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -X PATCH -d "{\"active\":\"true\",\"ftk_only\":\"true\",\"token_auth\":\"true\",\"token_type\":\"ftm\",\"ftm_act_method\":\"email\"}" -H "Content-Type:application/json" https://172.30.71.174/api/v1/ldapusers/8/"

Step 11 Flowchart 3: Pass LDAP Username and OTP to FAC to authenticate

curl -k -v -u "admin-api:mQZNoRBqESfnRfXsTfvfX3vlEEmdgbaBNrjBhWGJ" -d "{\"username\":\"davidr\",\"token_code\":\"376928\"}" -H "Content-Type:application/json" https://172.30.71.174/api/v1/auth/

Response: Success

HTTP/1.1 200 OK

Response: Failed

HTTP/1.1 401 UNAUTHORIZED
< Date: Wed, 06 Jan 2016 22:45:26 GMT
< Server: Apache
< Vary: Accept,Accept-Language,Cookie
< X-Frame-Options: SAMEORIGIN
< Content-Language: en
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=utf-8

User authentication failed* Connection #0 to host 172.30.71.174 left intact

Response: Failed, Token locked

HTTP/1.1 401 UNAUTHORIZED
< Date: Wed, 06 Jan 2016 22:45:31 GMT
< Server: Apache
< Vary: Accept,Accept-Language,Cookie
< X-Frame-Options: SAMEORIGIN
< Content-Language: en
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=utf-8

User is locked* Connection #0 to host 172.30.71.174 left intact

Sample Content for Message Displays

Flowchart 2

Step 3: “User not found. Please try again. If error persists, contact your System Administrator.”

Step 4: “Please input your mobile number to be able to use token self-service in the future. Number format must be +[international number]. For example +14085551234.”

Step 11: “A new FortiToken Mobile token has been assigned to you. Check your email to activate your token and then enter token code to login.”

Flowchart 3

Step 1: Prompt user to enter OTP or to Request a New Token.

Step 15: “Your account has been locked due to too many failed attempts. Please try again in a few minutes.”

Step 8: “Error: [*put error message returned from FAC here*] - Please try again. If error persists, contact your System Administrator.”

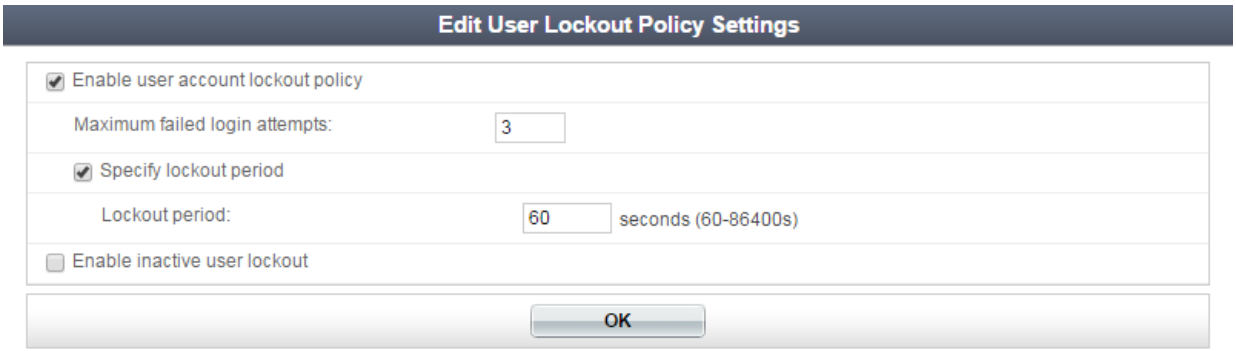
Step 4: “Please input your mobile number to be able to use token self-service in the future. Number format must be +[*international number*]. For example +14085551234.”

Step 10: “A token code is required to access Mantis from an external IP address. A new FortiToken Mobile token has been assigned to you. Check your email to activate your token and then enter token code to login.”

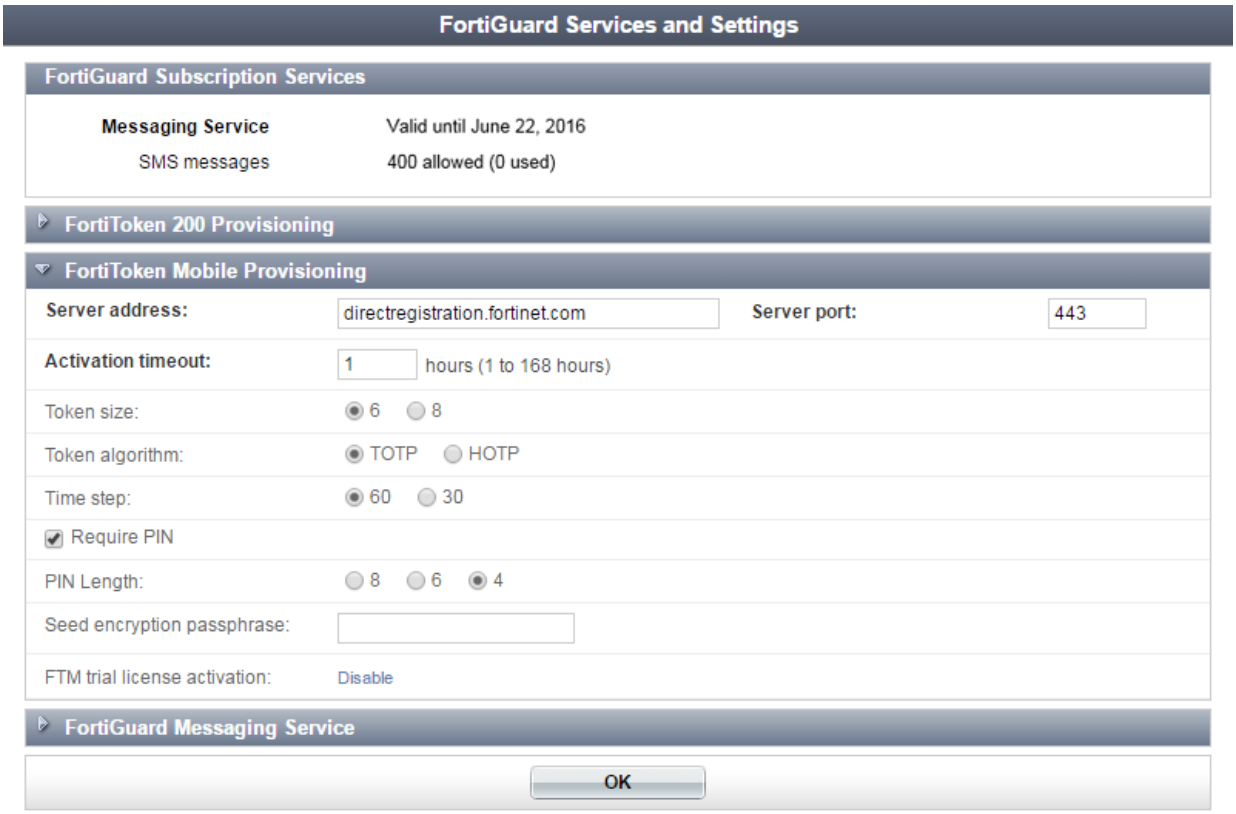
FAC Admin UI Settings

This section contains some useful suggestions for optional settings in FAC for the type of application described in this guide.

- Go to **Authentication > User Account Policies > Lockouts**. The image below shows the default values for **User Lockout Policy Settings**:
  - **Enable user account lockout policy**:It is recommended to keep this setting enabled.
  - **Maximum failed login attempts**: A higher value than the default is recommended (e.g. **10**).



- Go to **System > Administration > FortiGuard**. The image below shows the default settings found under **FortiToken Mobile Provisioning**:
  - **Activation Timeout:** A higher timeout is recommended for this type of application (e.g. **168**).
  - **PIN Policy:** If enabled, the user will be forced to set a PIN for the mobile token app.
  - **Time Step:** As per Initiative for Open Authentication (OATH) recommendations, this value should be set to **30**.


FortiGuard Services and Settings
FortiGuard Subscription Services
Messaging Service
Valid until June 22, 2016
SMS messages
400 allowed (0 used)
FortiToken 200 Provisioning
FortiToken Mobile Provisioning
Server address:
directregistration.fortinet.com
Server port:
443
Activation timeout:
1
hours (1 to 168 hours)
Token size:
6
8
Token algorithm:
TOTP
HOTP
Time step:
60
30
Require PIN
PIN Length:
8
6
4
Seed encryption passphrase:
FTM trial license activation:
Disable
FortiGuard Messaging Service
OK